Three Lines of Defense vs Five Lines of Assurance: Elevating the role of the Board and CEO in Risk Governance

Tim J. Leech Managing Director Risk Oversight Solutions Inc.
Lauren C. Hanlon Director Risk Oversight Solutions Inc.

Business leaders are continuously exposed to a multitude of ideas, theories, and models that all claim will help them do a better job. One of the current trending corporate governance models that many boards of directors have been exposed to already, or will be soon, is called the THREE LINES OF DEFENSE model. The global Institute of Internal Auditors (IIA), national regulators, risk management associations, major consulting firms, and others are aggressively promoting, rallying behind it and, on the legal front, even starting to legislate it. A groundswell of global support for this model is building. Be warned however, this chapter and its authors offer a word of caution - The THREE LINES OF DEFENSE model is based on traditional governance methods that have not worked well in tens of thousands of cases, and does not respond well to emerging expectations that call on CEOs and boards to more actively and visibly participate in and oversee their company's risk governance framework.

This chapter provides an overview of the THREE LINES OF DEFENSE risk governance movement; overviews some of the contrarian positions; outlines sub-optimal, even dangerous, elements of the THREE LINES approach; and then proposes a framework that boards of directors, C-suites, legislators, regulators, professional associations, consultants and others should carefully consider as a superior alternative if the goal is better corporate governance, increasing shareholder wealth, and national prosperity - the FIVE LINES OF ASSURANCE risk governance framework.

THE ORIGINS OF THE THREE LINES OF DEFENSE ("3LOD") MODEL

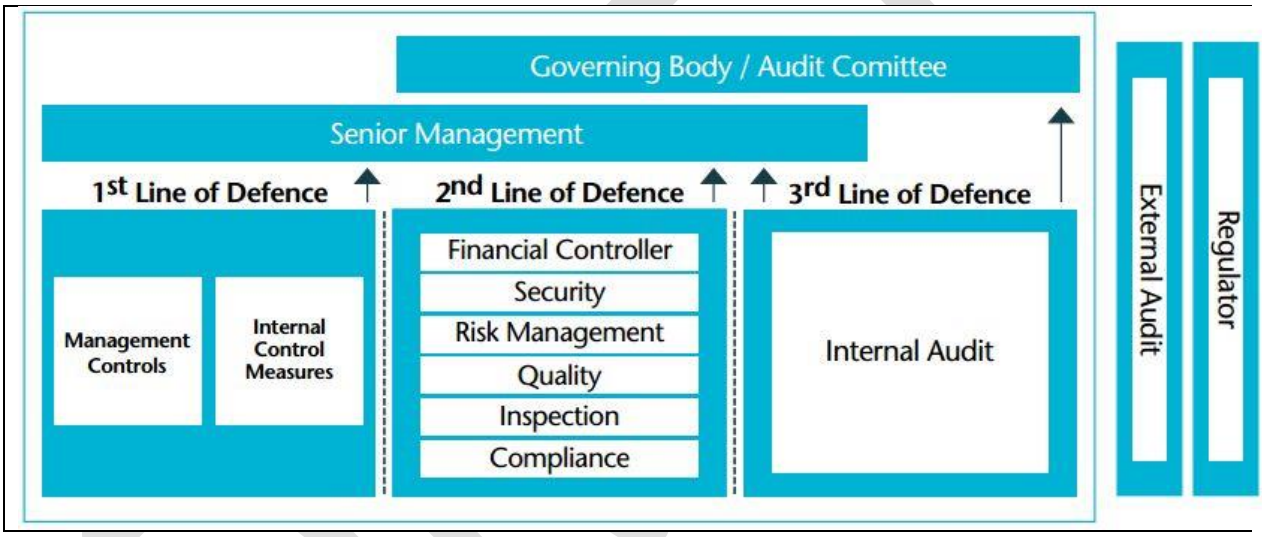
The general notion of multiple lines of defence has been around for centuries. Throughout history battle leaders regularly considered the need to use multiple lines of defence to protect positions they wanted to hold. Although the idea of three lines of defence in risk governance has been around since the 1990's, in January 2013, with the rise of formalized risk management and the increased use of dedicated enterprise risk management (ERM) groups driven by the 2008 global financial crisis and wary financial regulators, the IIA produced a position paper titled "The Three Lines of Defense in Effective Risk Management and Control". A paragraph in the introduction of the paper summarizes why the authors believe a model is required:

It's not enough that the various risk and control functions exist – the challenge is to assign specific roles and to coordinate effectively and efficiently among these groups so that there neither "gaps" in controls nor unnecessary duplication of coverage. Clear responsibilities must be defined so that each group of risk and control professionals understands the boundaries of

their responsibilities and how their positions fit into the organization's overall risk and control structure.

The stakes are high. Without a cohesive, coordinated approach, limited risk and control resources may not be deployed effectively, and significant risks may not be identified or managed appropriately. In the worst cases, communications among the various groups may devolve to little more than an ongoing debate about whose job it is to accomplish specific tasks.

The IIA paper introduces the model with the visual shown in Table ZZZ-1 below that the authors indicate was adapted from a paper produced by the European Confederation of the Institute of Internal Auditors titled "Guidance on the 8th Company Law directive, Article 41". In many ways, the 2013 IIA 3LOD paper described what was already status quo in a large percentage of major public companies.



It is important to note that the IIA paper sees senior management and boards as oversights of the three lines of defense, not active participants or additional "lines of defence".

Governing bodies and senior management are the primary stakeholders served by the "lines" and they are the parties best positioned to help ensure that the Three Lines of Defense model is reflected in the organization's risk management processes. (page 2)

The three "lines" are distinguished at a high level in the IIA paper as:

- Functions that own and manage risks
- Functions that oversee risks
- Functions that provide independent assurance

Later in the paper this is further defined as:

- Risk Owners/Managers
- Risk Control and Compliance
- Risk Assurance

The 1st line's responsibilities are summarized on page 3 as "Operational management identifies, assesses, controls, and mitigates risk" It isn't clear why, but the paper does not see the 1st line formally reporting upwards on risk status after they have assessed risk to the C-Suite or board of directors.

The 2nd line includes staff functions that are involved in some way with what management does on an ongoing basis. The 2nd line's primary purpose is summarized on page 2 as "Management establishes these functions to ensure that the first line of defense is properly designed, in place, and operating as intended"

The role of the 3rd line of defence, internal audit, is defined on page 5 as follows:

Internal audit provides assurance on the effectiveness of governance, risk management, and internal controls, including the manner in which the first and second lines of defense achieve risk management and control objectives.

The European Community Institute of Internal Auditors ("ECIIA"), the group that first proposed the three lines of defense framework, summarized the roles of the three lines in a posting on the IIA Norway website as follows:

- *As a first line of defence, the organisation's operational management has ownership, responsibility and accountability for assessing, controlling and mitigating risks.*
- *As a second line of defence, the risk management function (and also other supporting functions like compliance, quality) facilitates and monitors the implementation of effective risk management practices by operational management and assist the risk owners in reporting adequate risk related information up and down the organisation.*
- *As a third line of defence, the internal auditing function will, through a risk based approach, provide assurance to the organisation's board and senior management, on how effective the organisation assesses and manages its risks, including the manner in which the first and second lines of defence operate. This assurance task covers all elements of an organisation's risk management framework: i.e. from risk identification, risk assessment and - response to communication of risk related information.*

It is important to note that the authors of the ECIIA paper, like the authors of the IIA discussion paper issued later in 2013, did not see management in the first line of defence formally reporting upwards on risk status after assessing risk or, if they did, it isn't stated.

Since the Three Lines of Defense paper was published in January 2013 the IIA has taken aggressive steps to elevate and promote the model globally. The IIA's "Global Advocacy Platform" paper that all IIA members are encouraged to share and promote to internal audit stakeholders includes in Principle 2.2 the following:

Organization management is responsible for designing and operating an effective system of risk management and internal control. The "Three Lines of Defense" (3LoD) model provides valid guidance on clear accountability for risk management and internal control. (see also Appendix B)

The October 2015 issue of Internal Auditor magazine's feature story is titled "Defense in depth: Organizations that have adopted the three lines model experience collaborative opportunities to address risk." The laudatory article includes the following rationale on page 28 for relegating senior management and the board to oversight positions as opposed to assigning them active risk governance line roles:

The IIA's model does not include the board of directors and equivalent governing bodies or senior management among the lines of defense. Instead, they are considered stakeholders served by the three lines. However, because they are responsible for setting organizational objectives and establishing structures to manage any risks arising the pursuit of those objectives, they play an important role in risk and control.

Overall, it is puzzling to the authors why the IIA continues to exclude the board of directors as a line of defense in the model. Based on the number of lawsuits shareholders have directed at boards, particularly in the U.S., the authors can clearly state that a large percentage of shareholders view the board of directors as the ultimate line of defense.

REGULATORY ENDORSEMENTS TO DATE

Financial regulators around the world are grappling with how to best revise their oversight guidance and inspection systems to prevent a reoccurrence of the 2008 financial crisis.

A 2014 Institute of International Finance paper titled "IIF WGOR Feedback on the "Three Lines of Defense Model" summarized the evolution of financial sector acceptance of 3LOD in the introduction:

The Basel Committee on Banking Supervision's Principles for Sound Management of Operational Risk (BCBS PSMOR, June 2011) first mentioned the three lines of defense concept as applied to operational risk management, but it was somewhat ambiguous about whether the model was being required.[2] However, the Financial Stability Board's Progress Report to the G20 on Increasing the Intensity and Effectiveness of SIFI Supervision (FSB report, November 2012) and the specific questions on the model included in the recent BCBS stock-taking survey on PSMOR clarified and reinforced that message.

Footnote 2 referenced in the paragraph above reads:

Paragraphs 13 to 17 of the PSMOR, for example, mention the three lines of defense model only as a "common industry practice"; however, paragraph 32 (Principle 5 on role of Senior Management) seems to indicate that it is THE required approach.

Office of Supervision of Financial Institutions ("OSFI"), Canada's primary financial regulator, signalled that they like the simplicity of the accountability system embedded in the 3LOD model. This was graphically demonstrated in their August 2015 exposure draft "Operational Risk Management". The exposure draft proposes making 3LOD a core principle that all Canadian financials regulated by OSFI must adopt. The draft principle OSFI proposed is shown below.

4. Three Lines of Defence
Principle 3: FRFIs ensure effective accountability for operational risk management. A 'three lines of defence' approach, or appropriately robust structure, serves to separate the key practices of operational risk management and provide adequate independent overview and challenge. How this is operationalized in practice in terms of the organisational structure of a FRFI will depend on its business model and risk profile.

The OSFI August 2015 exposure draft describes very specific roles for each of the three lines of defence that go well beyond the generalities outlined in the 2013 IIA position paper, but is still largely based on traditional risk governance and assurance methods. Of particular note is the first line of defence description which, unlike some of the earlier papers on 3LOD, including the 2013 IIA discussion paper, OSFI does envision the first line of defence reporting upwards on residual operational risk. Unfortunately, OSFI does not state that a primary role of the second line should be to assist the first line to assess and report on the state of risk, nor does it state that a key role of the third line should be to assess and report on the reliability of the first line of defence's residual risk report, as well as the efforts of the second line to assist and quality assure the first line's efforts.

Financial regulators in other countries have already followed, or are expected soon in the absence of a radical change in direction to directionally follow the 3LOD path Canada has proposed in response to Basel Committee and FSB recommendations.

A high level review of Canadian, U.S. and UK stock exchanges requirements completed by the author in November 2015 did not disclose any specific requirements, expectations or comments. Financial sector public companies, influenced by the Basel Committee on Banking Supervision and Financial Stability Board comments have already begun to reference 3LOD in their SEC 10K disclosures. An example of a disclosure from Allied Irish Bank in a U.S. 10K filing is shown below in Table ZZZ-2.

2.3 Risk governance and risk management organisation

The Board and senior management have ultimate responsibility for the governance of all risk taking activity in the Group. AIB uses a 'three lines of defence' framework in the delineation of accountabilities for risk governance.

Under the three lines of defence model, primary responsibility for risk management lies with line management. Line management is supported by three Group and Divisional functions with a risk governance role. These are the enterprise-wide Risk, Regulatory Compliance and Finance functions. Together these act as the second line of defence. The third and final line of

defence is the Group Internal Audit function which provides independent assurance to the Audit Committee of the Board on all risk-taking activity.

Source:
http://secfilings.nyse.com/filing.php?ipage=6213881&DSEQ=&SEQ=66&SQDESC=SECTION_PAGE, page 65

3LOD CONTRARIAN POSITIONS

Because a growing number of risk and assurance experts and thought leaders have serious reservations about the 3LOD approach a formal debate forum was organized in the UK in the fall of 2014. The stated purpose was to debate the motion "The Three Lines of Defence philosophy is not fit for purpose". A newsletter titled Audit and Risk Chartered Institute of Internal Auditors dated January 6, 2015 summarized the results of that debate. Debate positions are summarized in Table ZZZ- 3 below:

Points for the motion included:

- The three lines of defence model is not a philosophy, but it is an old outdated concept.
- It is a concept that has little to offer in terms of the practical human experience in complex organisations and is an absurd simplification of real life.
- It is a model that has been imposed by regulators, whom we now do our best to please. The internal audit community has adopted it for the sake of a simple life.
- The Parliamentary Commission on Banking concluded that this "philosophy" isn't fit for purpose.

Points against the motion noted:

- The three lines of defence model is a brilliant philosophy. What could be simpler than having the people who take the risk in the first line, the people who monitor the people taking the risk in the second line and then people who check what the first line and the second line are doing in the third line?
- It is a philosophy that has stood the test of time and that perhaps reduces risk management to a simple endeavour that simple people can understand.
- It is a philosophy that is very much alive.

The article concluded with "A final vote was taken as the debate closed and the motion was defeated by 24 votes to 20 – a 30 per cent swing that suggests that the debate is far from over."

In July of 2014 Norman Marks, one of a handful of global risk and audit experts that regularly writes, blogs, tweets and covers global developments in the risk governance space authored a

blog post in “Norman Marks on Governance, Risk Management, and Audit”. Marks’ blog post describing his concerns with 3LOD, is shown below in Table ZZZ-4.

Risk Management is not about Defense

July 28, 2014

From time to time, I get into trouble with the IIA.

Here's another opportunity.

The IIA has embraced the Three Lines of Defense Model and in 2013 issued a Position Paper (identified as *strongly recommended guidance*) The Three Lines of Defense in Effective Risk Management and Control. Since then, IIA leadership has advocated the model, including in its recent Enhancing value Through collaboration: A call to action (see this related post).

The idea of the model has some merit. It distinguishes between functions that own and manage risk (operational management: the 1st line of defense), those that "oversee risk" (including risk management facilitation and monitoring of risk management practices: the 2nd line of defense), and those who provide independent assurance (primarily internal audit: the 3rd line of defense). Distinguishing the roles of management, risk management, and internal audit has merit. It is also useful to talk about the need for coordination.

However, I believe the IIA has made a grave mistake.

Risk management is not about *defense*.

It's about management making informed decisions and taking the right risks.

If anything, that is *offense*.

Defense implies you are defending against risk. If you don't take risk, you wither and die.

Defense implies that risk is bad. It is not. It can be positive or negative and, as one sage individual commented on my blog, there is often an opportunity to change a potential negative into a positive.

Last week, I met a top financial services risk management expert in Singapore (Martin Davies of Causal Capital). He told me about a situation where a trader submitted a proposed transaction for risk management review and approval. It was rejected because it fell outside the organization's "risk appetite" (used in this context, it really referred to risk criteria rather than risk appetite as defined by COSO ERM). The risk manager rejected it. Martin explained how if he were in this situation he would sit down with the trader and work with him on how the deal could be restructured such that it is acceptable.

This is offense, not defense.

In any event, my view is that when you put responsibility for managing risk in the hands of a siloed risk management function you are at the same time removing that responsibility from operating management.

This is not a good thing.

Management needs to own risk, with risk management serving as facilitator.

The IIA paper talks about risk management "overseeing" and "monitoring" risk management practices – which sounds awfully (and I mean awful in every sense) like corporate police and a siloed, adversarial risk management function.

No. This is a practice that will only stifle an organization and limit achievement.

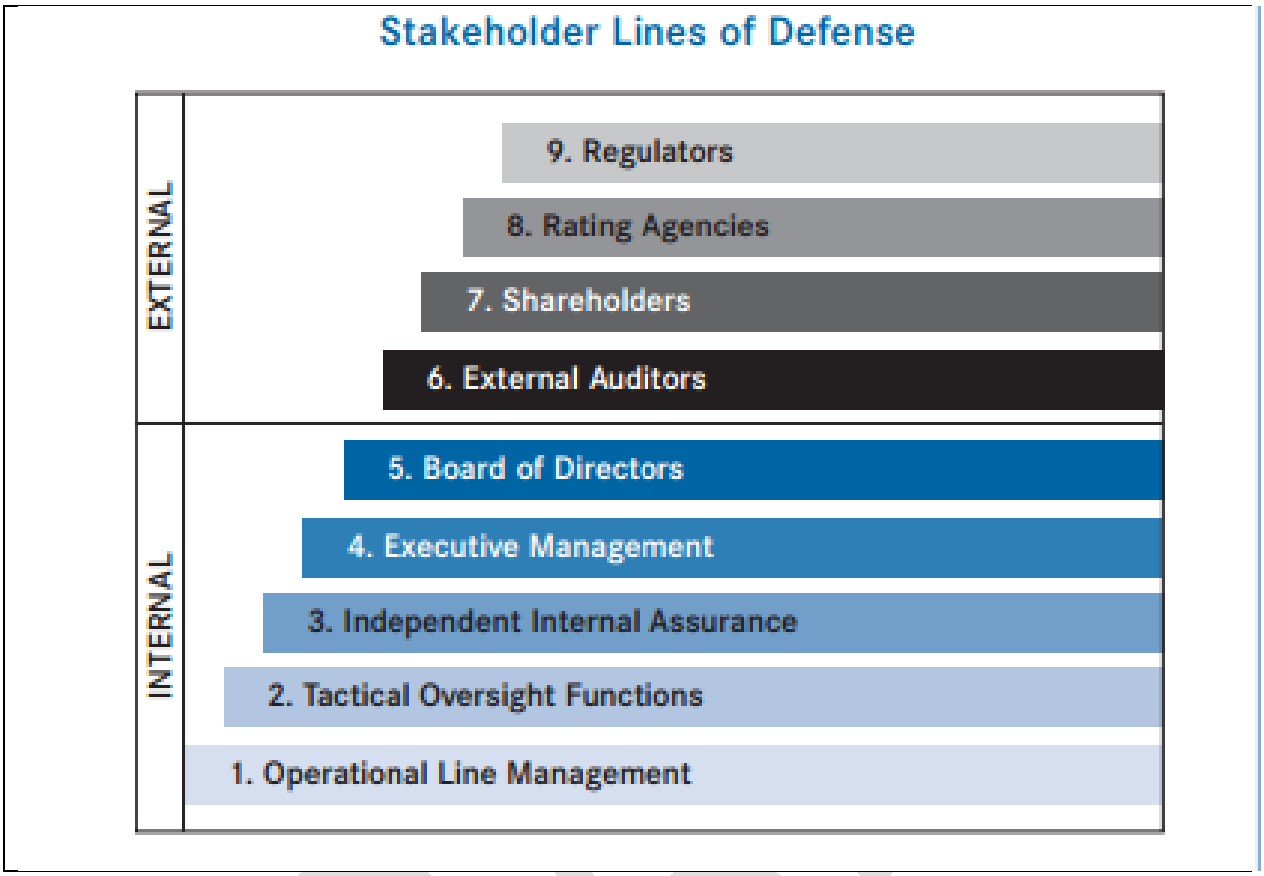
Let's talk about the lines of offense instead of defense.

How can risk management enable the organization to take the right risks, optimize outcomes, and not only achieve but surpass objectives?

I welcome your comments.

Prior to the issuance of the IIA paper in 2013 a number of risk and assurance practitioners had begun to promote the view that it should be FIVE LINES OF DEFENSE not 3LOD. Although there may be more risk and assurance experts around the world calling for senior management and the board to be added to the 3LOD model as key lines that the authors aren't aware of, the most noted calls for their inclusion have come from the global consultancy Protiviti in their 2013 news bulletin titled "Applying Five Lines of Defense Managing Risk"; and Sean Lyons in a much earlier October 2011 Conference Board paper titled "Corporate Oversight and Stakeholder Lines of Defense".

Table ZZZ-6 below drawn from Sean Lyons' Conference Board October 2011 paper illustrates the expansion of two additional internal lines of defence and four additional external lines of stakeholder defence.



SUBOPTIMAL/EVEN DANGEROUS ELEMENTS OF 3LOD

In a response to the Canadian financial regulator's August 2015 exposure draft on operational risk proposing to mandate 3LOD, Tim Leech, one of this chapter's authors organized his objections to 3LOD under three headings – FRAMEWORK NOMENCLATURE, TECHNICAL SUPPORT FOR FIVE LINES OF ASSURANCE and FINANCIAL STABILITY BOARD SUPPORT FOR FIVE LINES OF ASSURANCE. His October 8, 2015 comment letter calls on OSFI to modify their guidance and replace 3LOD with FIVE LINES OF ASSURANCE. Excerpts from Leech's October 2015 comment letter are reproduced below:

Framework Nomenclature

Contemporary risk governance professionals around the world promote the view that risk management and risk governance is fundamentally about increasing certainty that key objectives will be achieved while still operating within acceptable levels of residual risk. This interpretation flows from the ISO 31000 risk management standard definition of the word "risk" – the effect of uncertainty of achieving objectives. Using the ISO definition of risk objectives

covered should include an organization's key value creation/strategic objectives, as well as objectives which have potential to significantly erode value.

I believe that the word "DEFENCE" used in the framework promoted in the OSFI ED connotes a heavy emphasis on hazard avoidance, a stigma attached to the discipline of risk management that many risk professionals are trying to change. In the sporting world teams that only practice defense as opposed to a balance of offence and defense won't score many goals and win games. A key role of risk management is to help senior management and boards decide on appropriate balance of resources between creating value and driving profits and complying with applicable laws and regulations to create wealth, drive national and international prosperity, and stay within social norms of acceptable conduct. Unfortunately, surveys indicate that boards of directors have been slow to apply formal risk management methods to strategic planning processes as they don't see the connection. One can argue that the 2008 financial crisis is rooted in flawed strategy adopted by a large number of significant financial firms. While I recognize that laws and regulations in the financial sector are heavily skewed to protecting the international and national economies as well as a range of stakeholders impacted by activities of financial institutions, I believe that national regulators also have a role to play promoting value creation and enhancing the wealth and well-being of national economies. This is best achieved by requiring and promoting the use of frameworks that promote a careful balancing of value creation and value protection.

Technical Support For Five Lines Of Assurance

Not long after efforts began to elevate the THREE LINES OF DEFENSE approach, an approach coined and promoted by the Institute of Internal Auditors in 2013 and others earlier (see https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf) Protiviti, an international consulting firm, and others have, in essence, suggested that the THREE LINES OF DEFENSE model is incomplete and suboptimal at best, conceptually flawed at worst. A simple Google search on the term FIVE LINES OF DEFENSE quickly points to some of this debate and the key differences between the THREE LINES OF DEFENSE and what has been coined the FIVE LINES OF DEFENSE. The main difference in the FIVE LINES OF DEFENSE proposals are the addition of key roles identified for senior management and the board of directors. A link to a short bulletin published by Protiviti that describes the key elements of what they reference as FIVE LINES OF DEFENSE can be found at http://www.protiviti.ca/en-US/Documents/Newsletters/Bulletin/The-Bulletin-Vol-5-Issue-4-Applying-5-Lines-Defense-Managing-Risk-Protiviti.pdf. Given the huge importance of the role played by the C-Suite and board of directors in an effective risk governance framework, it would seem to make sense that regulators use every possible opportunity to elevate the risk governance roles and responsibilities of those two groups.

Financial Stability Board Support For Five Lines Of Defense/Assurance

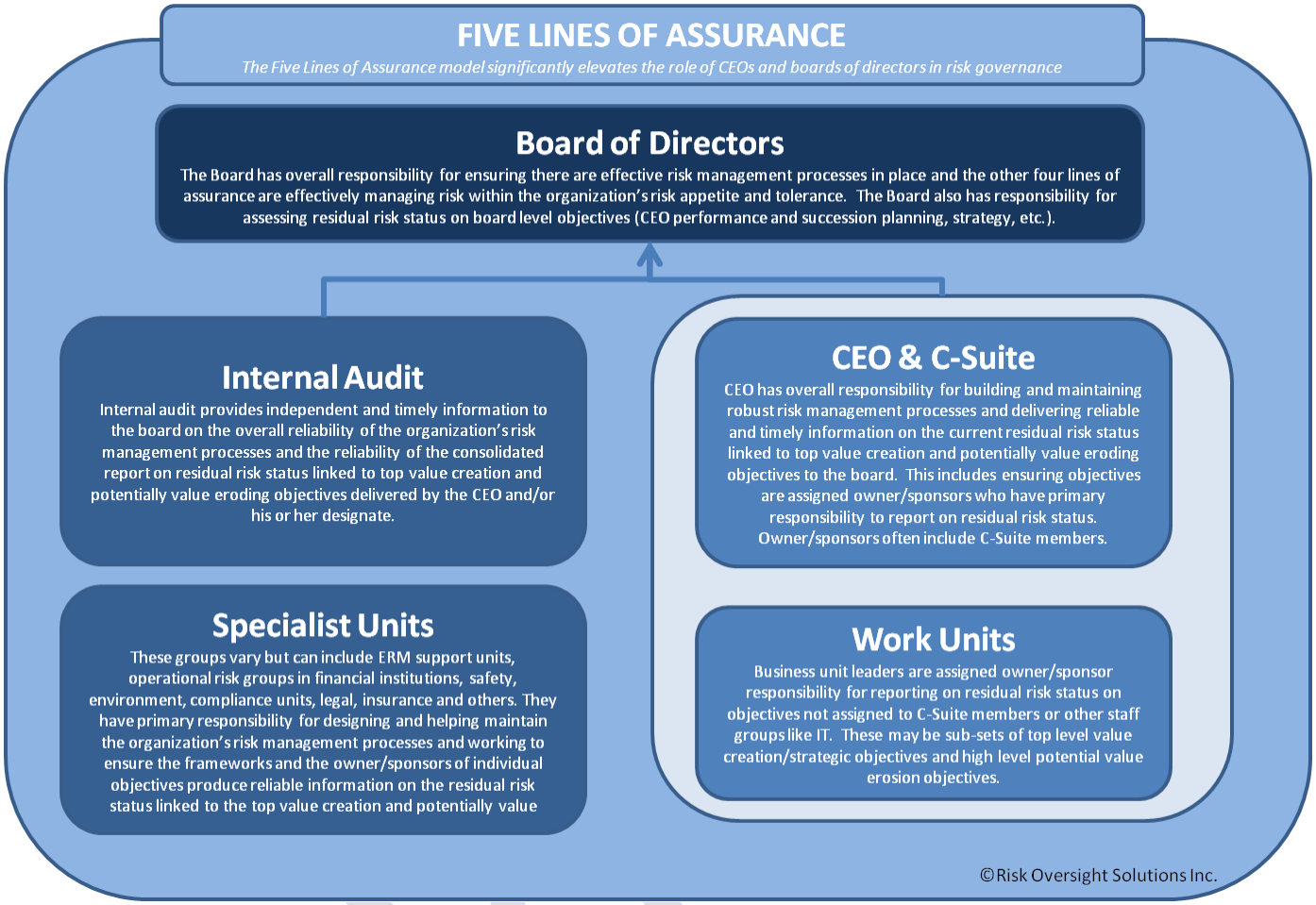
As OSFI is no doubt very well aware as a result of active participation of OSFI staff, current and past, and the role of Mark Carney past Governor of Bank of Canada, current Governor Bank of

England, and Chair of Financial Stability Board (FSB), the FSB has published a number of truly ground-breaking papers describing the changes FSB believes national regulators should make to prevent a reoccurrence of the 2008 global financial crisis. One of those papers is the seminal November 2013 ***Principals for An Effective Risk Appetite Framework.*** (http://www.financialstabilityboard.org/wp-content/uploads/r_131118.pdf) Pages 8 and 9 of that document do a great job articulating the risk governance roles that should be played by Chief Executive Officers and the Board of Directors. My analysis of the work of the FSB since it was constituted is that the FSB is, in fact, promoting a five line of assurance framework as key to achieving optimal results and preventing future financial crisis and global instability.

FIVE LINES OF ASSURANCE – WHAT IS IT?

The FIVE LINES OF ASSURANCE model is a superior alternative to 3LOD and is closely aligned to the FIVE LINES OF DEFENSE framework being promoted by Sean Lyons and Protiviti noted earlier with some key differences. The most obvious difference is the use of the word "ASSURANCE" as a replacement for "DEFENSE". This is not an insignificant difference. Focusing risk management and assurance around value creation objectives is just as important as, if not more important, than focusing on value erosion. The authors believe that corporate governance is fundamentally about balancing the interests of competing stakeholders and deciding how to best allocate resources to stay within the entity's risk appetite and tolerance in the pursuit of its objectives. National economies and their residents depend on companies to take risks in the pursuit of value creation which, in turn, helps drive national prosperity. Promoting risk governance models that put disproportionate focus on DEFENSE is not aligned with this goal.

A comprehensive description of all elements of the FIVE LINES OF ASSURANCE approach is beyond the scope of what can be accomplished here, but a diagram overview of some of the key 3LOD differentiators is below in Diagram ZZZ-6



The authors' recommendation for FIVE LINES OF ASSURANCE builds on the foundation of an objective centric risk management approach. A summary of key elements of Risk Oversight Solutions' BOARD & C-SUITE DRIVEN/OBJECTIVE CENTRIC ERM & INTERNAL AUDIT approach to FIVE LINES OF ASSURANCE drawn from a June 2015 Conference Board Director Notes paper authored by Parveen Gupta and Tim Leech titled THE NEXT FRONTIER FOR BOARDS: OVERSIGHT OF RISK CULTURE is shown below. More detailed information on the core elements of Board & C-Suite driven/Objective Centric ERM and internal audit is available on the Risk Oversight Solutions' website.

Board & C-suite Driven/Objective-centric ERM: Core Elements

Core element #1 Use an objectives register. Use an end-result OBJECTIVES REGISTER as the foundation building block for all ERM and assurance work done by the board, senior management, work units, internal audit, ERM teams, safety, compliance, environment and other

assurance groups. This simple step elevates two core reasons for using ERM: 1) to increase the certainty that important objectives will be achieved operating within a level of residual risk status acceptable to senior management and the board, and 2) to provide reliable information to help boards and senior management make better resource allocation decisions.

Core element #2 Active board/senior management involvement and cost/benefit analysis. The OBJECTIVES REGISTER should, at a minimum, include the organization's top value creation/strategic objectives and the top potential value erosion objectives (i.e. objectives where non-achievement significantly erodes entity value). This ensures that ERM integrates with strategic planning, performance evaluation and remuneration, as well as key safety, compliance and IT security initiatives. ERM and related formal assurance work consume time and money. Senior management and the board should play an active role defining which end-result objectives warrant the time and resources formal risk management requires and how much. The OBJECTIVES REGISTER plays a key role fostering better board/C-suite-driven assurance. This simple step has great potential to integrate the work of all of the "assurance silos" and increase board risk oversight transparency.

Core element #3 Clear accountability. Traditional ERM methods often focus on identifying RISK OWNERS for each risk. This approach calls for identification of an OWNER/SPONSOR for each objective selected for inclusion in the OBJECTIVES REGISTER. An objective OWNER/SPONSOR may, or may not, decide that it makes sense to assign RISK OWNERS for some or all of the significant risks that increase uncertainty a specific objective will be achieved. However the OWNER/SPONSOR retains overall responsibility for reporting upwards on RESIDUAL RISK STATUS linked to their business objective(s), not just the status of individual risks covered in more traditional risk registers. A key question that should be asked is, "Why would we assign 'risk owners' if there is no clarity/visibility on who owns and/or has responsibility for the related end result business objective?"

Core element #4 Define risk assessment rigor and independent assurance levels. For each objective included in the OBJECTIVES REGISTER a RISK OVERSIGHT COMMITTEE comprised of senior management, with board oversight, should define how much risk assessment rigor and the amount/intensity of independent assurance senior management and the board believe is warranted. These decisions provide a clear roadmap for the ERM team, internal audit, and other assurance providers.

Core element #5 Consider the full range of risk treatments. Properly applied, ERM should identify and assess the full range or risk treatments, including risk financing/insurance, risk transfer/sharing/contractual indemnities, risk avoidance options; as well as risk mitigation techniques, often more narrowly referenced as "internal controls." This requires input from auditors, insurance specialists, legal advisors, line management, senior management, and the board. Sometimes the best way to treat a risk is to change the objective, which may even mean exiting the business sector. Many risk-centric approaches that use risk registers do not identify the full range of risk treatments; instead they focus primarily on "internal controls." This can produce dangerous and wrong conclusions on acceptability of residual risk.

Core element #6 Focus on acceptability of composite residual risk status. The objective-centric approach to ERM and internal audit produces a composite set of information called Residual Risk Status for each objective. This includes details on current and past objective performance, impact of not achieving the objective (as opposed to impact(s) linked to a single risk), any impediments that create barriers for the objective owner/sponsor to adjust residual risk

status, and "concerns"—situations where a viable risk is not being treated in whole or in part. Concern data can also include information on viable risk treatments not currently in use/place that could further reduce residual risk status. Owner/Sponsors, senior management and the board use this information to help assess the acceptability of the current residual risk status. This information provides a tangible basis for identifying an organization's real risk appetite/tolerance and better allocating resources.

Core element #7 Optimize risk treatments. Once a decision has been made by the OWNER/SPONSOR with oversight from senior management and the board on the acceptability of residual risk status, the entity can consider whether the current combination of risk treatments is "optimized" – i.e. the lowest cost possible combination of risk treatments capable of producing an acceptable residual risk status. Traditional ERM methods may not emphasize evaluating risk treatment optimization/cost reduction opportunities. Risk-centric processes driven by risk registers make this step difficult as the full range or risks that impact the certainty specific objectives will be achieved are not identified and evaluated in composite and the full range of risk treatments available is not considered.

FIVE LINES OF ASSURANCE – WHY IS IT BETTER?

The IIA globally and many national financial regulators appear to be coalescing around the 3LOD approach in spite of the many serious negatives identified by its critics to date. Directors, and the associations that represent them such as NACD in the U.S., ICD in Canada, and IoD in the UK have largely been silent on the 3LOD issue. This could be because directors don't see any direct impacts on boards from the 3LOD proposals as it is largely already status quo in their organizations, or alternatively in litigious cultures, directors may be content with not being specifically identified by the IIA 3LOD model as an active participant who must ensure they are receiving reliable and timely information on the state of residual risk related to key objectives from CEOs, but merely recipients of risk status information from management. A highly summarized list of benefits of adopting FIVE LINES OF ASSURANCE as a superior alternative to 3LOD closes out this chapter.

Benefits of FIVE LINES OF ASSURANCE vs 3LOD

Benefit #1 – Boards are active participants not bystanders. Boards are squarely assigned responsibility for overseeing the effectiveness of risk management processes in the companies they represent and completing risk assessments on the handful of core objectives that they are directly responsible for. One objective that boards are, or should be, directly responsible for includes the absolutely key objective of ensuring that the CEO and CFO are operating the company within the risk appetite and tolerances established by the board. The process also provides a tangible platform that allows boards to actively participate in the process to develop, refine, and modify key strategic objectives, specify risk assessment rigor and independent

assurance levels, and to ensure that risk assessments with the specified rigor and assurances have been completed on those objectives.

Benefit #2 – CEOs are directly responsible for reporting on residual risk status to the board. Unlike the 3LOD which sees no active risk governance role for CEOs, this approach assigns direct responsibility to CEOs for establishing reliable risk management processes and providing their boards with regular and reliable enterprise level reports on residual risk status linked to key strategic/value creation objectives and potentially value eroding objectives.

Benefit #3 – Emphasis is on balancing offense and defense. Teams that only focus on defense don't score many goals. National prosperity and creation of shareholder wealth depends on prudent risk taking in the pursuit of objectives. The word defense perpetuates negative stereotypes of risk management that have often caused risk managers to be seen as the "Office of NO", not a function that has potential to help management increase certainty key objectives will be obtained while still operating within an acceptable level of retained risk.

Benefit #4 – It is consistent with the Financial Stability Board (FSB) paper titled "Principles for Effective Risk Appetite Frameworks". In the authors' experience the best regulatory produced paper on risk management to date is the 2013 FSB paper "Principles for Effective Risk Appetite Frameworks". That paper, starting on page 8, defines active and key roles for the board, CEOs, specialists groups, business units and internal audit. The approach proposed by the FSB in that paper is closely aligned with the FIVE LINES OF ASSURANCE approach proposed in this chapter.

Benefit #5 – Internal audit's role and stature are elevated. With some exceptions, the role seen for internal audit in many of the 3LOD papers is largely an endorsement of the status quo role of internal audit functions – selecting and planning audits, completing audits, and reporting results of those audits each year on a small fraction of the total risk universe. The 2013 IIA 3LOD paper does not suggest that management self-assess risks to the top value creation and potentially value eroding objectives and provide a consolidated report on the state of residual risk to the board. Since formal management reporting to the board on risk status isn't an expectation in the IIA 3LOD approach, internal audit is not expected to provide boards with independent assurance that management's report on risk status linked to top objectives is reliable. (i.e. there is no report from management on the state of risk so IA can't opine on what doesn't exist) The role for internal audit envisioned in FIVE LINES OF ASSURANCE elevates IA to one of being a key assurance provider to the board on the risk status reports the board receives from management on the full range of top value creation and potentially value eroding objectives.

Benefit #6 – Role of risk specialists is clearly defined. When using the FIVE LINES OF ASSURANCE approach the mandate of risk support groups is clear –assist the company and senior management implement and maintain processes capable of producing reliable consolidated reports on residual risk status linked to top value creation and potentially value eroding objectives necessary for long term success for senior management and the board; and helping management optimize risk treatment strategies (i.e. the lowest cost possible combination of risk treatments capable of producing an acceptable level of residual risk)

Benefit #7 – Optimizing risk treatments is a key goal. Unfortunately, traditional internal audit departments that complete spot-in-time audits on a small fraction of the risk universe and risk-centric ERM processes that use risk registers as their foundation don't focus much attention, if any, on ensuring that the current risk treatment design is optimized – i.e. the lowest possible cost combination of risk treatments capable of producing an acceptable level of residual risk linked to key objectives. This is a key benefit that audit and risk specialists need to embrace and promote as a major value adding service they provide.

Benefit #8 – Over time the word "control" will be replaced with "risk treatments". The origins of the word "control" is closely linked to accounting and financial audits. As a general statement controls only cover things that are focused on mitigating risk likelihood and/or consequence. Controls do not include what risk professionals call "risk financing" strategies including insurance; risk sharing/transfer strategies often represented by contract clauses and indemnities designed to treat specific risks; risk avoidance strategies; and, perhaps most importantly, traditional processes don't directly encourage careful and prudent acceptance of some risks. Effective risk management requires prudent management and board choices on how to best treat the major risks to top value creation and potentially value eroding objectives.

Benefit #9 – Regulators send a key message – CEOs and Boards must play key risk governance roles. Unlike the FSB guidance Principles for Effective Risk Appetite Frameworks and the UK Corporate Governance Code that call on boards to actively take steps to satisfy themselves they are receiving reliable information on the true state of residual risk status linked to key objectives from management; the 3LOD framework, perhaps by design, sees a limited role for CEOs and senior management; and only an oversight role for Boards. History tells us that many of the most important risk acceptance decisions occur at the C-Suite and Board levels.

Benefit #10 – Supports better resource allocation decisions. In the final analysis, good governance is about making good decisions on where and how to allocate limited resources in the pursuit of an organization's objectives – objectives that often conflict. The FIVE LINES OF ASSURANCE approach better helps organizations and their boards accomplish that goal.

CONCLUDING REMARKS

Companies and their boards all around the world may soon face pressure from professional accounting and auditing associations, including the Institute of Internal Auditors; financial and securities regulators; and others to adopt the 3LOD approach to risk governance. This chapter represents a heart-felt plea from the authors based on decades of experience working with organizations that want more effective ERM and internal audit to do everything you can to resist calls to adopt 3LOD and, instead, actively promote the implementation of what is referenced generally in this chapter as the FIVE LINES OF ASSURANCE approach to risk governance – a vastly superior approach.

REFERENCES

Financial Stability Board, 2013, Principles for An Effective Risk Appetite Framework, 18 November 2013, http://www.financialstabilityboard.org/wp-content/uploads/r_131118.pdf

Gupta, P, Leech, T, 2015, The Next Frontier for Boards: Oversight of Risk Culture, Conference Board Director Notes, June 2015, https://www.conference-board.org/publications/publicationdetail.cfm?publicationid=2962

Institute of Internal Auditors, January 2013, IIA Position Paper: THE THREE LINES OF DEFENSE IN EFFECTIVE RISK MANAGEMENT AND CONTROL, https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf (November 3, 2015 link)

Institute of Internal Auditors Norway, Web posting, http://www.iia.no/The+ECIIA+endorses+the+three+lines+of+defence+model+for+internal+governance.9UFRrQ4T.ips, (November 3, 2015 link)

Institute of Internal Auditors, Undated, Global Advocacy Platform, https://na.theiia.org/about-ia/PublicDocuments/Global%20Advocacy%20Platform.pdf (November 3, 2015 link)

Institute of International Finance, March 2014 and June 2014, IIF WGOR Feedback on the "Three Lines of Defense Model: IIF First 3LOD Paper and IIF Second 3LOD Paper, https://www.iif.com/news/regulatory-affairs/iif-wgor-identifies-challenges-implementing-three-lines-defense-model-orm (November 3, 2015 link)

Leech, T, 2015, Risk Oversight Solutions comment letter to OSFI, October 8, 2015 http://riskoversightsolutions.com/wp-content/uploads/2011/03/Risk-Oversight-Solutions-Tim-Leech-Response-to-OSFI-E-21-ED-Op-Risk-Mgmt-Oct-8-2015.pdf (November 4, 2015 link)

Lyons, S, 2011, Corporate Oversight and Stakeholder Lines of Defense, Conference Board Executive Action Series, October 2011, https://www.google.com/#q=corporate+oversight+and+stakeholder+lines+of+defense, (November 3, 2015 link)

Marks, N, 2014, Risk Management is not about Defense, personal blog Norman Marks on Governance, Risk Management and Audit, July 28, 2014, https://normanmarks.wordpress.com/2014/07/28/risk-management-is-not-about-defense/ (November 3, 2015 link)

Marks, N, Further Thoughts on the Three Lines of Defense Model, October 14, 2015, https://normanmarks.wordpress.com/2015/10/14/further-thoughts-on-the-three-lines-of-defense-model/ (November 3, 2015 link)

News, Audit and Risk: Insights from the Chartered Institute of Internal Auditors, 2015, http://auditandrisk.org.uk/news/experts-debate-three-lines-of-defence-model (November 3, 2015 link)

Office of the Superintendent of Financial Institutions, Operational Risk Management exposure draft, August 2015, http://www.osfi-bsif.gc.ca/Eng/Docs/e21.pdf (November 3, 2015 link)

Protiviti, 2013, The Bulletin, Applying the Five Lines of Defense in Managing Risk, Volume 5 Issue 4, http://www.protiviti.com/en-US/Documents/Newsletters/Bulletin/The-Bulletin-Vol-5-Issue-4-Applying-5-Lines-Defense-Managing-Risk-Protiviti.pdf (November 3, 2015 link)

Seago, J., 2015, Defense in depth: Organizatons that have adopted the three lines model experience collaborative opportunities to address risk, October 2015, page 26- 31, web access restricted to IIA members